(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平8－84140

(43)公開日　平成８年(1996) ３月26日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｈ０４Ｍ	3/42	Ｅ			
				Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願平6－217009

(22)出願日　平成６年(1994) ９月12日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　三鬼　準基
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　雲崎　清美
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

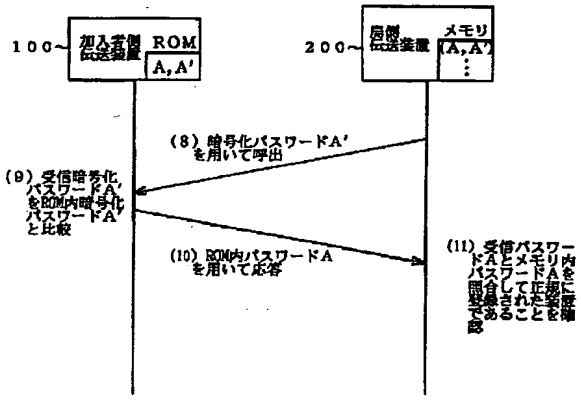
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　加入者認証方法

(57)【要約】

【目的】　安全性が高くかつ所要回路規模の少ない加入者認証を実現する。

【構成】　複数の加入者側装置１００が通信網を介して局側装置２００と結ばれ、局側装置は登録された加入者側装置にサービスを提供する。加入者側装置１００は、装置固有のパスワードＡと該パスワードＡを公開鍵で暗号化した暗号パスワードＡ′を保持し、そのうち、暗号パスワードＡ′を局側装置２００に登録する。局側装置２００は、各加入者側装置毎に、暗号パスワードＡ′とそれを秘密鍵で復号したパスワードＡを保持する。通信の開始時、局側装置２００はＡ′を用いて通信相手の加入者側装置１００を呼び出し、加入者側装置１００は、受信したＡ′と自己のＡ′を比較し、一致するとＡで応答し、局側装置２００は、受信したＡを保持してあるＡと照合する。



1

【特許請求の範囲】

【請求項１】　複数の加入者側伝送装置が通信ネットワークを介して局側伝送装置と結ばれ、局側伝送装置は登録された加入者側伝送装置にサービスを実施する登録加入者通信サービスシステムにおいて、加入者側伝送装置が局側伝送装置に正規に登録された装置であることを確認する加入者認証方法であって、

加入者側伝送装置は、各々、加入者側伝送装置を識別するための装置固有の秘密情報とネットワーク事業者から割り当てられた公開鍵で前記秘密情報を暗号化した暗号化情報とを保持するとともに、前記暗号化情報を局側伝送装置に登録し、

局側伝送装置は、各加入者側伝送装置について、加入者側伝送装置からの暗号化情報と該暗号化情報を秘密鍵により復号した復号情報とを組として保持し、

通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報と自己の暗号化情報とを比較して、一致する場合に自己の秘密情報を用いて応答し、局側伝送装置は加入者側伝送装置から送られてきた秘密情報を保持されている復号情報と照合することにより、通信相手の加入者側伝送装置が正規に登録された装置であることを確認することを特徴とする加入者認証方法。

【請求項２】　加入者側伝送装置の装置固有の秘密情報と、ネットワーク事業者から割り当てられた公開鍵で前記秘密情報を暗号化した暗号化情報とを組として、あらかじめ装置製造時または出荷時に個々の加入者側伝送装置内の読出し専用記憶素子（ＲＯＭ）に書き込んでおくことを特徴とする請求項１に記載の加入者認証方法。

【請求項３】　加入者側伝送装置はネットワーク事業者から割り当てられたＩＤ番号を設定する手段を有し、加入者側伝送装置の設置時に、局側伝送装置はＩＤ番号を用いて加入者側伝送装置の呼び出しを行い、加入者側伝送装置は局側伝送装置からのＩＤ番号と自己のＩＤ番号とを比較し、一致する場合、自己の暗号化情報を局側伝送装置へ送信して登録することを特徴とする請求項１に記載の加入者認証方法。

【請求項４】　通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報の一部あるいは全て、および局側伝送装置にあらかじめ登録したＩＤ番号を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報の一部あるいは全ておよびＩＤ番号と自己の暗号化情報およびＩＤ番号についてそれぞれ比較を行い、一致する場合に自己の秘密情報を用いて応答することを特徴とする請求項３に記載の加入者認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、一つの局側伝送装置と

2

複数の加入者側伝送装置が対向するポイント・ツー・マルチポイント形態の登録加入者通信サービスシステムにおける加入者認証方法に関するものである。

【０００２】

【従来の技術】図８は登録加入者通信サービスシステムの概略構成を示したもので、１００は加入者側伝送装置、２００は局側伝送装置、３００はネットワークオペレーションシステム、４００は加入者側伝送装置１００と局側伝送装置２００の間に介在するネットワーク網である。ネットワークオペレーションシステム３００は、加入者からの申告などによりサービスを許可する加入者側伝送装置１００を局側伝送装置２００に登録し、局側伝送装置２００は、この正規に登録された加入者側伝送装置１００に対して所望のサービスを実施する。なお、ネットワークオペレーションシステム３００は一般には複数の局側伝送装置を収容し、各局側伝送装置にそれぞれ複数の加入者側伝送装置がポイント・ツー・マルチポイント形態で接続されて、それぞれサービスエリアを形成している。

【０００３】従来、この種登録加入者通信サービスシステムにおける加入者認証方法は、個々の加入者側伝送装置に、その装置を識別するためのＩＤ番号と正規に登録された装置であることを証明するためのパスワードを割り当て、加入者側伝送装置に内蔵されたＲＯＭ（Read Only Memory)とネットワーク事業者の所有するデータベースに書き込む方式を採っていた。図６および図７により、従来の加入者認証手順の例を説明する。

【０００４】図６は登録時の手順を示したもので、まず、ネットワーク事業者がＩＤ番号とパスワードの対を大量に生成し（1）、データベースに蓄積する（2）。次に、これを伝送装置の製造業者に知らせる（3）。製造業者は装置の製造時または出荷時に個々の加入者側伝送装置のＲＯＭにＩＤ番号とパスワードを１組書き込む（4）。加入者は、加入者側伝送装置を購入した後（5）、その装置のＩＤ番号をネットワークオペレーションシステムに登録する（6）。これは、通常は加入者が自伝送装置のＩＤ番号をネットワーク事業者に届けることで行われる。ネットワークオペレーションシステムは、登録されたＩＤ番号を元にデータベースの検索を行い（7）、対応するパスワードを読み出し（8）、局側伝送装置のメモリに、これらのＩＤ番号とパスワードを書き込む（9）。

【０００５】通信の開始時には、図７に示すように、毎回、局側伝送装置がＩＤ番号を用いて加入者側伝送装置を呼び出し（１０）、加入者側伝送装置はパスワードを用いて応答する（１１）。局側伝送装置は、メモリに記憶されているパスワードと受信したパスワードを照合することで、正規に登録された伝送装置であることを確認する（１２）。

【０００６】

3

【発明が解決しようとする課題】上記従来の加入者認識方法では、大量のＩＤ番号とパスワードを書き込むための大規模なデータベースを必要する問題がある。また、加入者側伝送装置、局側伝送装置、ネットワークオペレーションシステム、及びデータベースの各装置間の伝送は安全性が保証されている必要があるため、伝送装置は暗号化回路等の付加により回路規模が増大するという問題もある。

【０００７】本発明は、大規模なデータベースを必要とせず、なおかつ伝送装置の回路規模が少なくてすむ加入者認証方法を提供することにある。

【０００８】

【課題を解決するための手段】本発明の加入者認証方法は、各加入者側伝送装置は、加入者側伝送装置を識別するための装置固有の秘密情報（パスワード）Ａとネットワーク事業者から割り当てられた公開鍵Ｐで前記秘密情報Ａを暗号化した暗号化情報Ａ′とを保持するとともに、前記暗号化情報Ａ′を局側伝送装置に登録し、局側伝送装置は、各加入者側伝送装置について、加入者側伝送装置からの暗号化情報Ａ′と該暗号化情報Ａ′を秘密鍵Ｑにより復号した復号情報Ａとを組として保持し、通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報Ａ′を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報Ａ′と自己の暗号化情報Ａ′とを比較して、一致する場合に自己の秘密情報Ａを用いて応答し、局側伝送装置は加入者側伝送装置から送られてきた秘密情報Ａを保持されている復号情報Ａと照合することにより、通信相手の加入者側伝送装置が正規に登録された装置であることを確認することを特徴とする。

【０００９】また、本発明の加入者認証方法は、加入者側伝送装置の装置固有の秘密情報Ａと、ネットワーク事業者から割り当てられた公開鍵Ｐで前記秘密情報Ａを暗号化した暗号化情報Ａ′とを組として、あらかじめ装置製造時または出荷時に個々の加入者側伝送装置内の読出し専用記憶素子（ＲＯＭ）に書き込んでおくことを特徴とする。

【００１０】また、本発明の加入者認証方法は、加入者側伝送装置はネットワーク事業者から割り当てられたＩＤ番号を設定する手段を有し、加入者側伝送装置の設置時に、局側伝送装置はＩＤ番号を用いて加入者側伝送装置の呼び出しを行い、加入者側伝送装置は局側伝送装置からのＩＤ番号と自己のＩＤ番号とを比較し、一致する場合、自己の暗号化情報Ａ′を局側伝送装置へ送信して登録することを特徴とする。

【００１１】更には、本発明の加入者認証方法は、通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報Ａ′の一部あるいは全て、および局側伝送装置にあらかじめ登録した上記ＩＤ番号を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送

4

装置からの暗号化情報Ａ′の一部あるいは全ておよびＩＤ番号と自己の暗号化情報Ａ′およびＩＤ番号についてそれぞれ比較を行い、一致する場合に自己の秘密情報Ａを用いて応答することを特徴とする。

【００１２】

【作用】本発明は、公開鍵暗号方式の一方向性を利用して、製造業者に割り当てた公開鍵と暗号化された秘密情報（暗号化されたパスワード）だけでは元の秘密情報（パスワード）を解読できないことを保証しつつ、伝送装置自体には秘密情報（パスワード）の暗号化／復号化回路を不要にするものである。。

【００１３】公開鍵暗号方式を用いた暗号化は、通常、図９に示す様な形態で実施される。秘密情報（パスワード）Ａを公開鍵Ｐにより暗号化を行い、該暗号化情報Ａ′を安全でない伝送路を経由して送信する。暗号化情報Ａ′受け取った側は、秘密鍵Ｑを用いて元の秘密情報（パスワード）Ａを復号する。この公開鍵暗号方式の特徴は、暗号化情報Ａ′と公開鍵Ｐからは元の秘密情報Ａを解読することはできないということである。

【００１４】本発明では、この公開鍵暗号化方式を利用することにより、ＩＤとパスワードを予め記憶しておくための大規模なデータベースを必要とせず、また、秘密情報及びその暗号化情報をあらかじめ伝送装置に保持しておくことにより、伝送装置自体には秘密情報の暗号化／復号化回路は不要である。

【００１５】

【実施例】以下、本発明の実施例について図面を参照して説明する。

【００１６】〈実施例１〉これは請求項１および２に対応するものである。図１および図２により、本実施例の加入者認証手順を説明する。図１は登録時の手順を示したもので、まず、ネットワーク事業者は公開鍵Ｐとそれに対応する秘密鍵Ｑを生成する（１）。次に、秘密鍵Ｑはネットワークオペレーションシステム３００に登録し（２）、公開鍵Ｐを伝送装置の製造業者に知らせる（３）。製造業者は装置の製造時または出荷時に、装置固有の秘密情報であるパスワードＡを生成し、公開鍵Ｐを用いてこのパスワードＡを暗号化する。そして、個々の加入者側伝送装置１００のＲＯＭに、該装置固有のパスワードＡとその暗号化情報である暗号化パスワードＡ′を１組書き込む（４）。加入者は加入者側伝送装置１００を購入した後（５）、その装置の暗号化パスワードＡ′をネットワーク事業者に届け出て、ネットワークオペレーションシステム３００に登録する（６）。ネットワークオペレーションシステム３００は、登録された暗号化パスワードＡ′を秘密鍵Ｑを用いて元のパスワードＡに復号した後、局側伝送装置２００のメモリに、これら暗号化パスワードＡ′とその復号情報であるパスワードＡを組にして書き込む（７）。

【００１７】通信の開始時には、図２に示す様に毎回、

5

局側伝送装置２００が暗号化パスワードA′を用いて通信相手の加入者側伝送装置１００を呼び出す（8）。加入者側伝送装置１００は局側伝送装置２００からの暗号化パスワードA′を受信し、ROM内の自己の暗号化パスワードA′と比較を行い（9）、一致する場合は、局側伝送装置２００に対してROM内の自己のパスワードAを用いて応答する（10）。一致しない場合は応答しない。局側伝送装置２００は、メモリに記憶されている暗号化パスワードA′と対のパスワードAと受信したパスワードAを照合することで、正規に登録された加入者側伝送装置１００であることを確認する（11）。

【0018】本実施例の認証手順を用いた場合、公開鍵暗号方式が安全である限り、暗号化パスワードA′と公開鍵Pだけでは元のパスワードAを復号できないため、加入者側伝送装置１００のROMに書き込まれたパスワードAを盗み出すか、ネットワーク事業者の有する秘密鍵Qを盗み出さない限り、他の加入者になりすますことはできない。また、ID番号とパスワードを予め記憶しておくための大規模なデータベースを必要とせず、伝送装置１００，２００にも秘密情報（パスワード）の暗号化／復号化のための回路を必要としない。

【0019】〈実施例2〉これは請求項3および4に対応し、パスワードの登録を遠隔から自動的に行える様にするとともに、パスワードの安全性をさらに高めるものである。図3、図4および図5により、本実施例の加入者認証手順を説明する。

【0020】図3において、まず、ネットワーク事業者は公開鍵Pとそれに対応する秘密鍵Qを生成する（1）。次に、秘密鍵Qはネットワークオペレーションシステム３００に登録し（2）、公開鍵Pを伝送装置の製造業者に知らせる（3）。製造業者は伝送装置の製造時または出荷時に、装置固有の秘密情報であるパスワードAを生成し、公開鍵Pを用いてこのパスワードAを暗号化する。そして、個々の加入者側伝送装置１００のROMに、該装置固有のパスワードAとその暗号化情報である暗号化パスワードA′を1組書き込む（4）。ここで、加入者側伝送装置１００には、個々の加入者側伝送装置を区別するためのID番号を設定するスイッチ（数桁の数値を設定できるスイッチ）が具備されているとする。加入者は加入者側伝送装置１００を購入した後（5）、ネットワーク事業者からID番号の割り当てを受け（6）、加入者側伝送装置１００に設定する（7）。一方、ネットワーク事業者は、加入者に割り当てたID番号をネットワークオペレーションシステム３００を経由して局側伝送装置２００のメモリに登録する（8）。

【0021】図4は遠隔登録の手順を示したもので、加入者が加入者側伝送装置１００をネットワークに接続した際、局側伝送装置２００は、ID番号を用いて加入者側伝送装置１００の呼出しを行う（9）。加入者側伝送

6

装置１００は局側伝送装置２００から受信したID番号を自己のID番号と比較を行い（10）、一致する場合はROM内の自己の暗号化パスワードA′を用いて応答する（11）。一致しない場合は応答しない。局側伝送装置２００は、受信した暗号化パスワードA′をネットワークオペレーションシステム３００に送る（12）。ネットワークオペレーションシステム３００は秘密鍵Qを用いて、元のパスワードAを復号し（13）、局側伝送装置２００に返す（14）。局側伝送装置２００は、暗号化パスワードA′とその復号情報のパスワードAをIDと組にしてメモリに書き込む。

【0022】この様にして、本実施例では、ネットワーク事業者から割り当てられたID番号を設定した加入者側伝送装置をネットワークに接続するだけで自動的に加入者登録が行われる。

【0023】通信の開始時には、図5に示す様に、局側伝送装置２００がID番号と暗号化パスワードA′の一部あるいは全てを組み合わせた値を用いて、加入者側伝送装置１００を呼び出す（15）。加入者側伝送装置１００は、局側伝送装置２００からID番号および暗号化パスワードA′を受信して、スイッチに設定された自己のID番号およびROM内の暗号化パスワードA′をそれぞれ比較し（16）、一致する場合はパスワードAを用いて応答する（17）。一致しない場合は応答しない。局側伝送装置２００は、メモリに記憶されているパスワードAと受信したパスワードAを照合することで、正規に登録された加入者側伝送装置であることを確認する（18）。

【0024】既存の認証方式では、ID番号は、ネットワーク事業者がサービスを提供している全ての地域で加入者側伝送装置を一意に決定できる必要があったため、非常に多くの桁数が必要であった。本実施例では、加入者側伝送装置をネットワークに接続する最初の時に、そのローカルなネットワーク内で加入者側伝送装置を区別できれば良いため、ID番号は2～3桁程度で十分である。また、通信の開始時の加入者側伝送装置呼び出し時にID番号を併せて用いることにより、パスワードを一部のみ使用することが可能となるため、パスワードの安全性をさらに高められる。

【0025】以上、本発明の実施例を説明したが、これらの実施例は、パッシブダブルスター形光加入者線伝送方式の様に、上り方向は下り方向と違って他の加入者に盗聴される心配が無い様な場合に適している。もし、上り方向の伝送も安全でない場合は、パスワードを通常の秘密鍵暗号方式によって暗号化して送信することによって安全性を保つことができる。この場合、第二の実施例での最初の暗号化されたパスワードの送信の際には、さらなる暗号化は必要ない。このため、パスワード自体を秘密鍵暗号方式の秘密鍵として使用することもできる。

【0026】

7

【発明の効果】以上の説明から明らかな如く、本発明によれば、公開鍵暗号化方式の一方向性を利用して、安全性が高くかつ所要回路規模の少ない加入者認証を実現することができる。また、個々の加入者側伝送装置を区別するためのＩＤ番号を加入者側伝送装置に設定することにより、暗号化されたパスワードを加入者からの申告によりあらかじめ局側伝送装置に登録しておく代わりに、加入者側伝送装置の設置時に、局側伝送装置からの呼び出しで自動的に遠隔登録することができる。さらに、通信の開始時の加入者側伝送装置の呼び出しにＩＤ番号を併せて用いることにより、パスワードを一部のみ使用することが可能となるため、パスワードの安全性をさらに高めることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例のパスワード登録時の手順を説明する図である。

【図２】本発明の第１の実施例の通信開始時の手順を説明する図である。

8

【図３】本発明の第２の実施例のＩＤ番号登録時の手順を説明する図である。

【図４】本発明の第２の実施例のパスワード自動登録の手順を説明する図である。

【図５】本発明の第２の実施例の通信開始時の手順を説明する図である。

【図６】従来の加入者認証方式を説明する図である。

【図７】図６の続きを示す図である。

【図８】登録加入者通信サービスシステムの一例の概略構成を示す図である。

【図９】公開鍵暗号方式を説明する図である。

【符号の説明】

１００　加入者伝送装置
２００　局側伝送装置
３００　ネットワークオペレーションシステム
４００　ネットワーク

【図２】

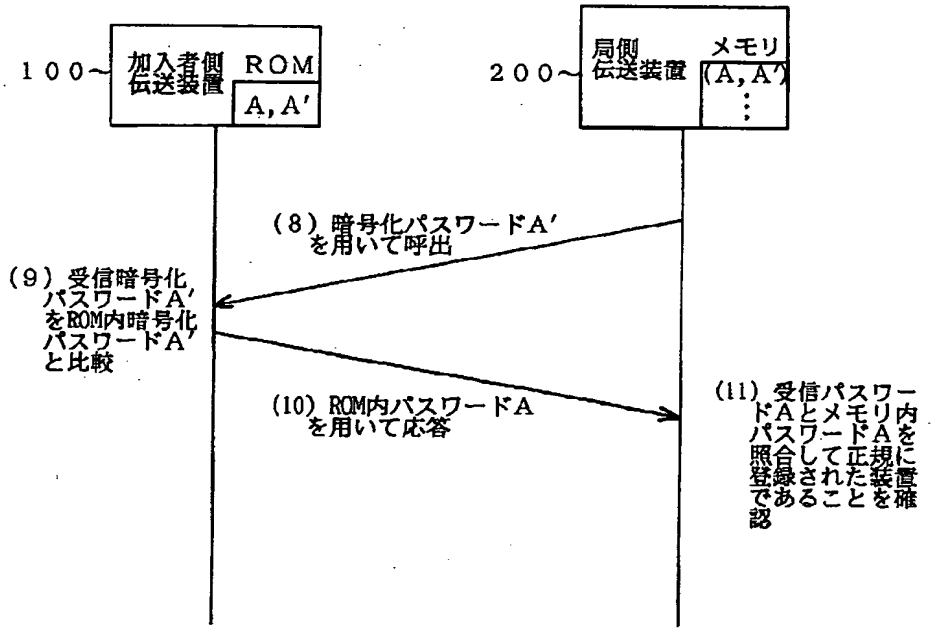
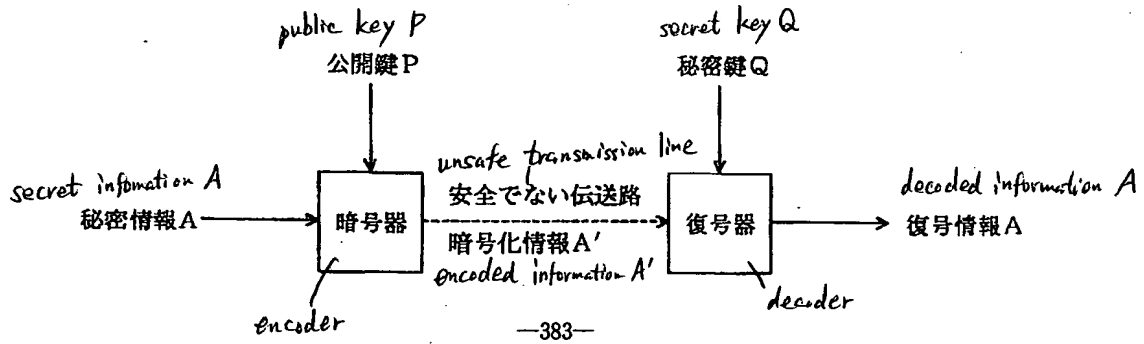
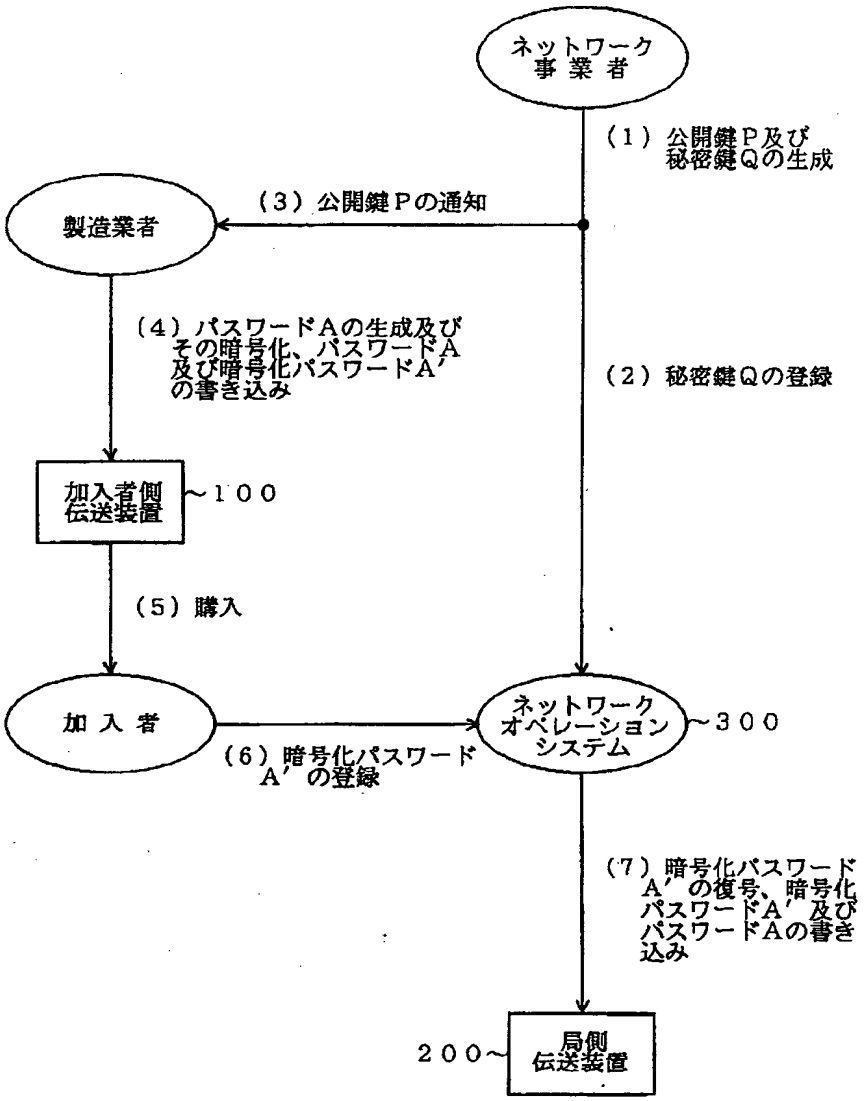


Fig. 9

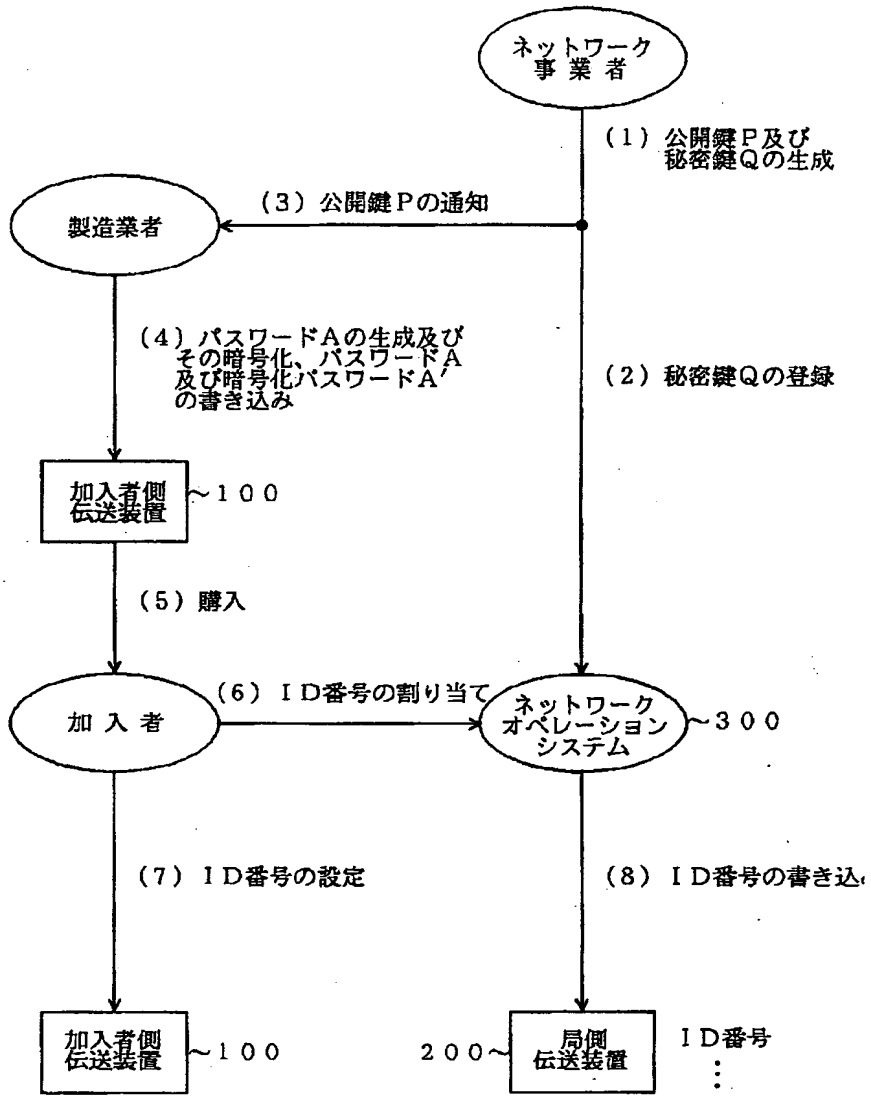
【図９】



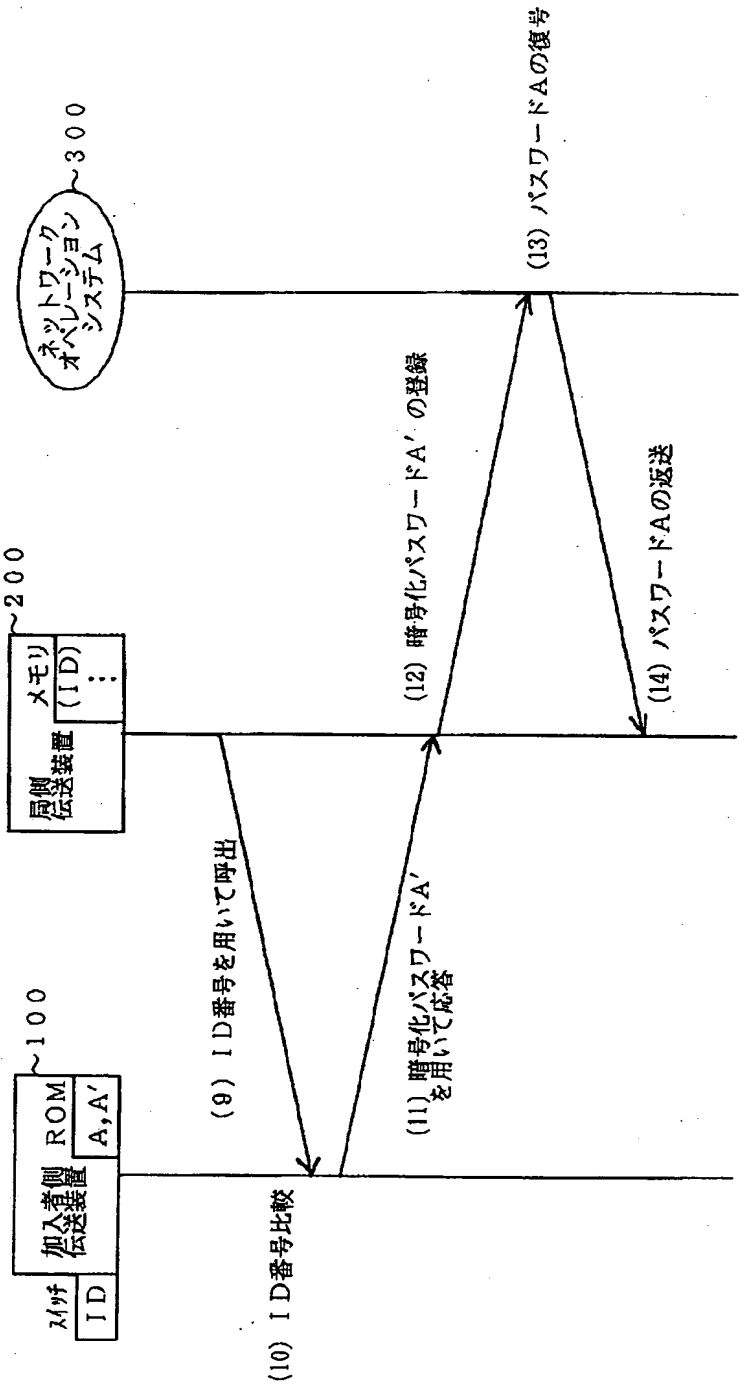
【図1】


ネットワーク事業者
(1) 公開鍵P及び秘密鍵Qの生成
製造業者
(3) 公開鍵Pの通知
(4) パスワードAの生成及びその暗号化、パスワードA及び暗号化パスワードA'の書き込み
(2) 秘密鍵Qの登録
加入者側伝送装置
100
(5) 購入
加入者
ネットワークオペレーションシステム
300
(6) 暗号化パスワードA'の登録
(7) 暗号化パスワードA'の復号、暗号化パスワードA'及びパスワードAの書き込み
200
局側伝送装置

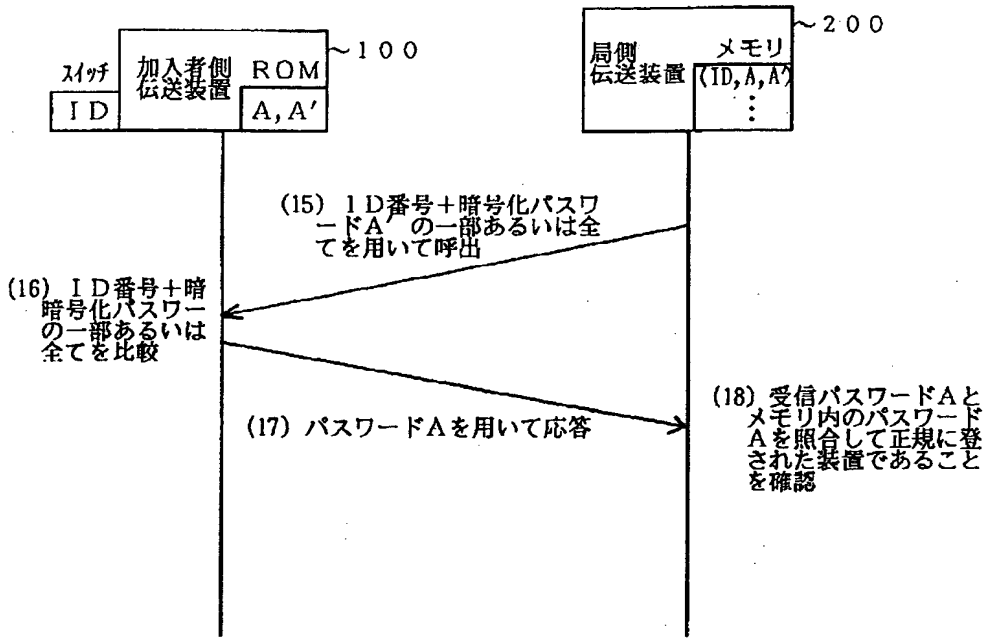
【図3】


ネットワーク事業者
(1) 公開鍵P及び秘密鍵Qの生成
製造業者
(3) 公開鍵Pの通知
(4) パスワードAの生成及びその暗号化、パスワードA及び暗号化パスワードA'の書き込み
(2) 秘密鍵Qの登録
加入者側伝送装置
100
(5) 購入
加入者
(6) ID番号の割り当て
ネットワークオペレーションシステム
300
(7) ID番号の設定
(8) ID番号の書き込
加入者側伝送装置
100
200
局側伝送装置
ID番号

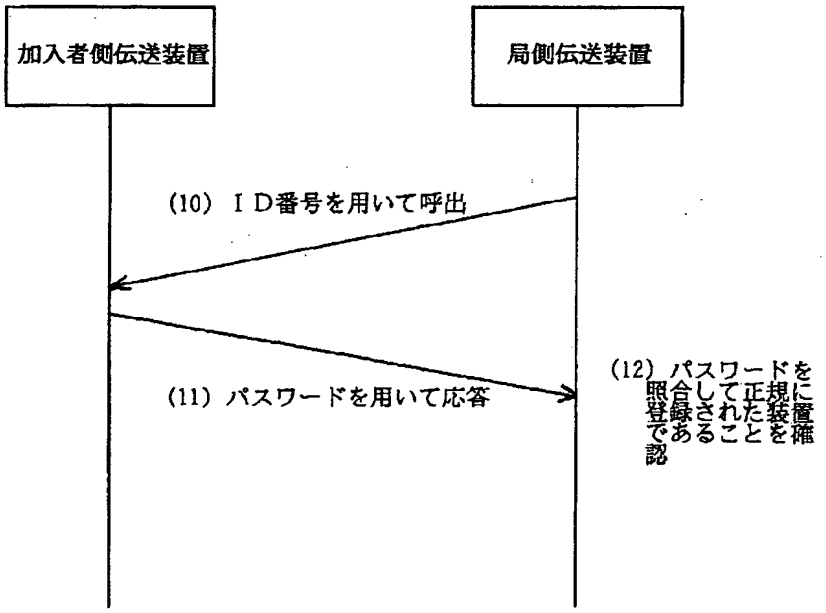
【図４】


ネットワーク
オペレーション
システム
300
(13) パスワードAの復号
200
局側
伝送装置
メモリ
(ID)
(12) 暗号化パスワードA′の登録
(14) パスワードAの返送
(9) ID番号を用いて呼出
(11) 暗号化パスワードA′
を用いて応答
100
加入者側
伝送装置
ROM
A,A′
メモリ
ID
(10) ID番号比較

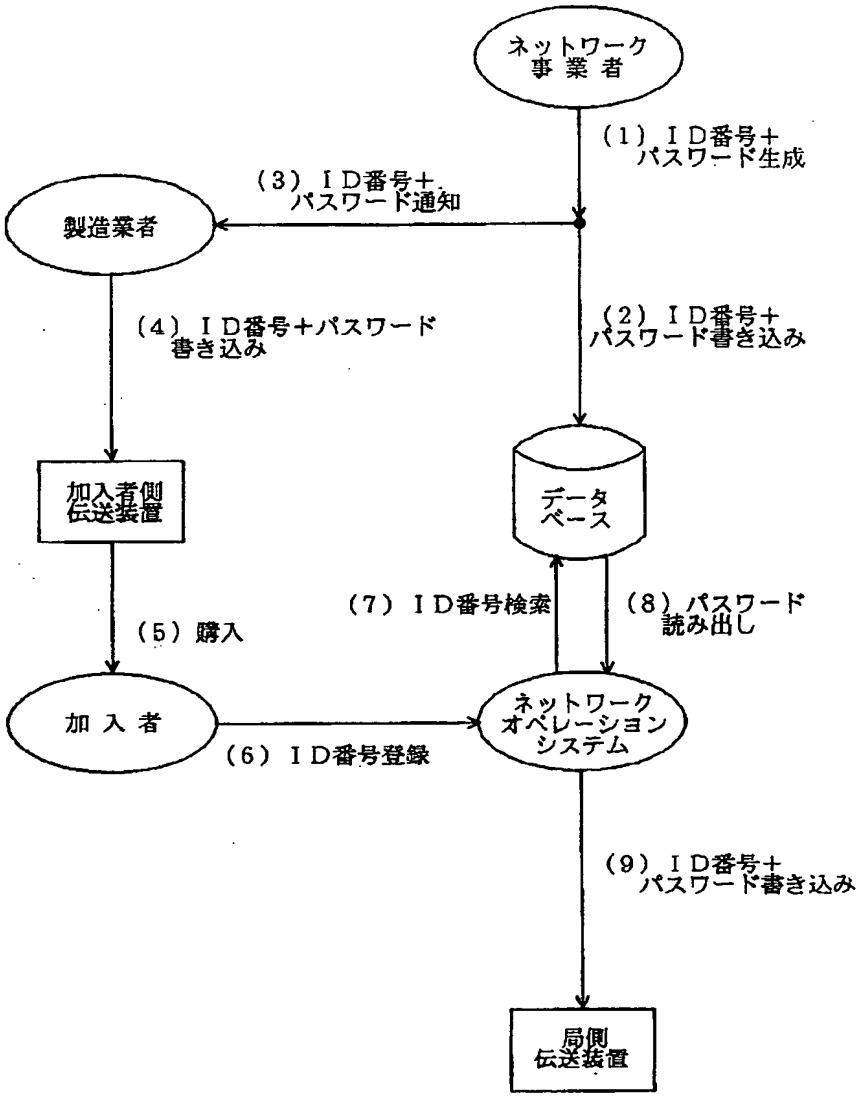
【図５】


スイッチ
ＩＤ
加入者側伝送装置
ROM
A, A′
～１００
局側伝送装置
メモリ
(ID, A, A′)
～２００
(15) ＩＤ番号＋暗号化パスワードA′の一部あるいは全てを用いて呼出
(16) ＩＤ番号＋暗号化パスワードの一部あるいは全てを比較
(17) パスワードＡを用いて応答
(18) 受信パスワードＡとメモリ内のパスワードＡを照合して正規に登録された装置であることを確認

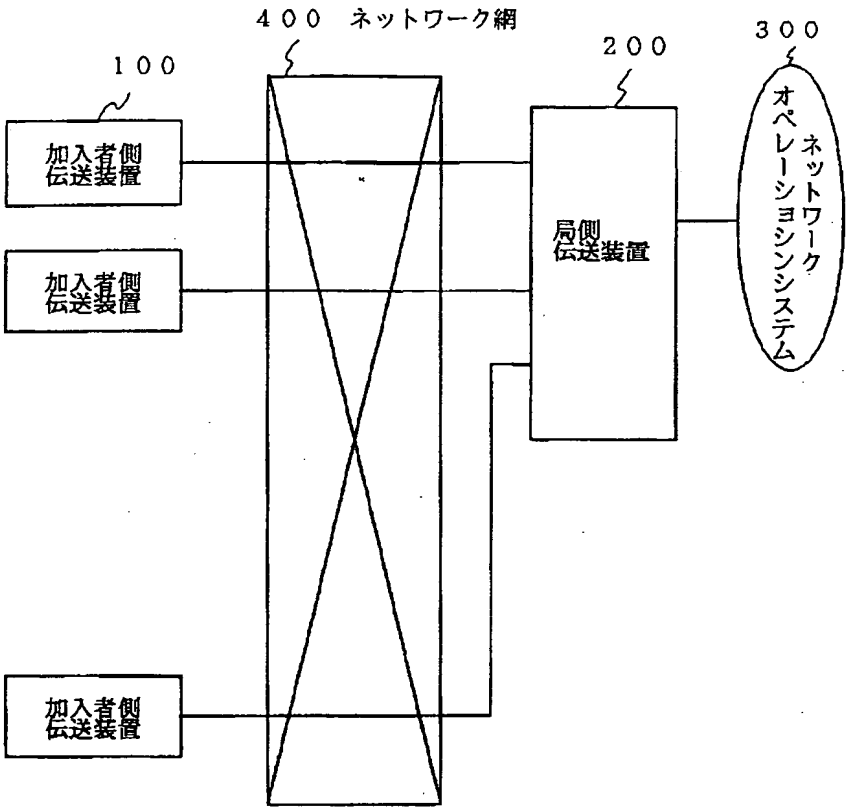
【図７】


加入者側伝送装置
局側伝送装置
(10) ＩＤ番号を用いて呼出
(11) パスワードを用いて応答
(12) パスワードを照合して正規に登録された装置であることを確認

【図６】


ネットワーク
事業者
(1) ＩＤ番号＋
パスワード生成
(3) ＩＤ番号＋
パスワード通知
製造業者
(4) ＩＤ番号＋パスワード
書き込み
(2) ＩＤ番号＋
パスワード書き込み
加入者側
伝送装置
データ
ベース
(7) ＩＤ番号検索
(8) パスワード
読み出し
(5) 購入
加 入 者
(6) ＩＤ番号登録
ネットワーク
オペレーション
システム
(9) ＩＤ番号＋
パスワード書き込み
局側
伝送装置

【図８】


４００　ネットワーク網
１００
２００
３００
加入者側伝送装置
加入者側伝送装置
加入者側伝送装置
局側伝送装置
ネットワークオペレーションシステム